Development of a Nuclear Plant Computer Aided Process Analysis and Management System

S.B. Guarro, J. Szabo, D. Okrent
University of California, MANE Dept., Los Angeles, California 90024, U.S.A.

Abstract

The development of a multi-function computer-aided process analysis and management (CAPAM) system, to be implemented in nuclear power plant control rooms, is discussed. The design goals identified for such a system are early disturbance detection and diagnosis, accompanied by identification of the best possible recovery actions or alternative success paths. Probabilistic safety margins to the loss of important safety functions may be also calculated. Two possible CAPAM concepts are illustrated, based on similar multi-level conceptual structures, but having different emphases in the development of their functional goals and utilizing different techniques for implementation. Possible approaches for validation of instrumentation signals to be used as inputs by a CAPAM system are also investigated.

1. Introduction

Design of a suitable structure for a Disturbance Analysis System (DAS) intended to cover a whole nuclear plant is a complex problem requiring consideration of many balancing factors. The evolution of DAS concepts has, since its early days, been oscillating between different definitions, from alarm analysis and prioritization strategies, to detection oriented systems based on advanced display and graphic techniques. Today a trend towards more complex and articulated systems is finally emerging. The objective is to achieve a better overall plant level of operational performance, through accomplishment of a set of integrated tasks [1-3].

For optimum and updated management of plant operations the following general problems must be addressed in the presence of a disturbance affecting one or more plant systems:

I) Early detection; the disturbance must be detected in the early stages, before it can produce irreversible consequences.

II) Early diagnosis; if possible, the root causes of the disturbance must be identified, so that the operator(s) have a good understanding of its likely course and may anticipate future consequences.

III) Identification of recovery actions; in most cases an early diagnosis will also allow the identification of simple recovery actions, which will eliminate the root causes of a disturbance and reverse its sequential course (e.g., if a system is not working because it has been valved out, the opening of the correct valve(s) will restore the proper process conditions).

IV) Identification of best available remedial actions; if recovery from an upset condition is not easily identifiable, alternative success paths to bring the plant process under safe controlled conditions must be readily identified and pursued.

In addition to the above, since the strategy for dealing with any abnormal set of conditions in a plant should be related to the overall goal of maintaining public risk at a minimum, it may also be desirable to calculate an on-line probabilistic operational risk measure. Thus, an additional useful task for an optimal plant operations

management system can be the calculation of the conditional probabilities of losing any important plant safety functions, given the occurrence of a disturbance.

This paper presents two alternative approaches to the development of an articulated, computer implemented system capable of performing all or most of the above tasks. In the following, we will conventionally refer to this computer implementation as CAPAM (Computer-Aided Process Analysis and Management).

2. CAPAM Multi-Level Structure

In the previous section we listed a few important objectives that should be achieved by an effective CAPAM system in the presence of a plant disturbance. For such a system to be truly effective these objectives will have to be pursued and coordinated according to a defined strategy, reflecting criteria that are at the basis of nuclear power plant (NPP) design and operation.

Reference [4] explains that the prime concern of NPP operators in post scram conditions must reside in assuring that certain specific "critical safety functions" be accomplished by the plant systems. This concept can be extended to pre-scram operations as well, by defining a suitable set of "operational safety functions" (OSFs). Reference [4] identifies four classes of post scram critical safety functions, of which the most fundamental is represented by the anti-core melt (ACM) safety functions. To categorize OSF's, one can follow a similar scheme, although some changes may be desirable in the definition of OSFs within each class. In the functional definition of the CAPAM systems, we elected to use, for a PWR plant, the following four ACM OSF's: 1) Reactivity Control (RC), 2) Core Heat Removal (CHR), 3) Primary Energy and Mass Inventory Control (PEMIC), 4) Reactor Coolant System Heat Removal (RCSHR).

The definition of "safety functions" allows one to construct a "top-down" conceptual model of plant operation from which the CAPAM objectives discussed in the previous section can be conveniently developed and prioritized. In any given plant, safety functions are accomplished by systems, which in turn are made up of subsystems and components. Failures or malfunctions at the component level can be relatively common, therefore it is important to rank the disturbances caused by these failures according to how serious a threat they represent to the plant. Response to different threats can thus be prioritized and attention can be devoted to solve the more serious problems first. Also important, in the presence of a disturbance, is to know if alternative success paths to achieve a threatened or compromised OSF are readily available, or if the root problem in the troubled system can be easily diagnosed and corrected.

To reflect the concepts illustrated above, the CAPAM structure that we propose is hierarchically articulated in three levels. Level One is the highest in hierarchy and provides the operator with a global picture of the plant OSF status. Level One actually draws information from the other two CAPAM levels, in order to identify threats to the plant OSFs and rank existing threats according to an assessment of their severity.

The CAPAM Level Two provides the operator(s) with more detailed information on the plant safety functions, by determining which success paths are available at any given time for accomplishing these. This same information is passed to Level One for the OSF threat severity assessment. The CAPAM Level Three contains the system detailed knowledge base and, on request, can provide more specific information on system or component status. It should be noted that the different degrees of operator support capability offered by the two CAPAM concepts presented in the following is largely determined by the different choices of system models adopted in their respective Level Three knowledge bases. The first CAPAM concept uses a "network-based" plant model, whereas the other is based on more conventional faul-tree/alarm-tree techniques, which, although quite less efficient and powerful, can in principle be adapted from existing PRA (Probabilistic Risk Assessment) analyses with some initial savings of labor and development costs.

3. Network-Based CAPAM

In the "Network-Based CAPAM" (NB-CAPAM) plant systems are modeled in Level-Three by means of Logic Flowgraph Methodology (LFM) networks [5]. The LFM technique allows the system analyst to develop a synthetic and effective graph representation of the cause-effect relations existing between plant physical parameters, control variables, protective devices and failure mechanisms. This graph representation is then stored in computer memory and can be automatically analyzed on line, in combination with input signals from the plant instrumentation, to produce "diagnostic trees" and "recovery trees". When a disturbance is in progress, these small boolean trees can in most cases exactly identify disturbance root causes, and, in addition, provide prescriptions on how to achieve system recovery without the use of alternative success paths (i.e., systems) for the affected OSF [6,7].

The detailed information provided by the LFM models can be of very high value to the plant operators, but, to be really useful, it must be accompanied by a properly defined frame of reference, which relates it to the global operational and safety goals represented by the plant OSF's. In order to achieve this, among all the physical process parameters and state variables that appear in the NB-CAPAM Level-Three models, the ones that more directly define the operability status of systems required to accomplish a safety function are identified and organized in the CAPAM Level-Two structure. This structure is essentially composed of truth tables representing the availability of systems and system trains. The Level-Two models can thus be used to identify which success paths are available at any time for the accomplishment of a particular OSF. This information can be directly accessed by the operator(s). In addition it is also accessed by the CAPAM Level One, which, based on the number of success paths made unavailable by a disturbance, comes up with an OSF threat severity assessment. The evaluation of OSF success path availability performed by use of the Level-Three and Level-Two models is also used as the starting point for calculation of probabilistic safety margins, as explanined in one of the next sections.

The actual development of the CAPAM models is obtained in a top-down fashion, starting with a definition of the plant OSF's, then continuing with the identification of success paths and systems that can be used within each OSF, and finally developing the LFM models for these systems (including all known important system interactions). Tables I, II and Figure 1 illustrate the concepts that we have just introduced. More specifically, Table I shows how the CAPAM Level One will assess the severity of a disturbance in terms of the fraction of success paths for the accomplishment of a given safety function that are made unavailable. Table II, in turn, shows a partial example of combinations of success paths available for the accomplishment of the PEMIC OSF in a PWR. This table represents an incomplete version of the truth tables to be employed by the CAPAM Level Two. The table shows that for a given OSF different sets of success paths will be available depending on the global plant operating state. The "Level-Two parameters" are essential parameters associated with a given OSF, and are used in the Level-Two truth tables for an additional and independent assessment of OSF status. Thus, if in a hypothetical situation both the pressurizer level and pressure are assessed to be "very low", the PEMIC OSF will be ranked as "threatened" in Level One, no matter how many success paths are presently shown to be available. The associated threat ranking scheme will be based on the size of the deviation of these parameters from the normal value and on the present plant operating state. As mentioned above, the systems and parameters tabulated in the CAPAM Level Two are modeled in detail in Level Three by means of LFM networks. Figure 1 shows an example of one such detailed model representing a PWR Pressurizer Level Control System. The reader interested in the details of LFM and in examples of how it can be utilized to produce diagnostic and recovery information is referred to Refs. [5] through [7].

In summary, the LFM models are used to assess the status of the Level-Two systems and parameters, which is in turn used by Level One for OSF status assessment. Level Three can also be directly accessed by the plant operators to obtain information on the root causes(s) of a disturbance and on possible measures for neutralizing its effects without calling on alternative success paths. Examples of both types of LFM use are given in the references cited above.

The information elaborated by the three CAPAM levels will be made available to the operators by means of an

Operational Safety Functional Panel (OSFP). This panel should consist of color CRTs, which will continually show OSF status by means of a color coded display in which each color represents the OSF threat severity rankings shown in Table I. This information will be integrated with a suitable CRT representation of Level-Two truth tables equivalent to the one pictured in Table II, showing which OSF success paths and systems are available or unavailable, and which essential parameters are affected under the plant prevailing conditions. The diagnostic and recovery information of Level Three will finally be displayed only if so requested by the operators. Note that Level-Three information will usually be available even for conditions that may fall short of being considered as an OSF "threat" by the CAPAM upper levels. This would be the case for any disturbances that would only cause minor degradation of plant systems and would not cause any major deviations in essential "Level-Two parameters". The continuous CAPAM Level-One and Level-Two CRT display will be provided with a window to alert the operators to the availability of more detailed CAPAM information in the Level-Three display, so that they can call it to the CRT screen if they so desire.

4. Fault-Tree-Based CAPAM

The second CAPAM concept that will be discussed here is essentially based on a "master fault tree" plant model similar to the one discussed in Ref. [8]. A CAPAM master tree must represent a core melt or severe core damage event in terms of loss of critical safety functions. Safety functions losses are further characterized formally in the tree in terms of system and system train losses. This makes it quite straightforward to derive from the master fault tree essentially the same type of information on safety function and system availability that was utilized in Levels One and Two of the NB-CAPAM discussed before. The two upper levels of the Fault Tree-Based CAPAM (FTB-CAPAM) can thus elaborate the same safety function threat severity and alternative success paths assessments that can be performed by the NB-CAPAM two upper levels. A useful extension of the features provided by the FTB-CAPAM Level Two can be obtained with the use of synoptical charts representing the execution of Emergency Procedure Guidelines (EPG's) to aid the operators in the material activation and alignment of alternative success paths when a threat to a given OSF is recognized. These charts could be in form and content similar to the EPG representation found in Ref. [9]. Limits on printing space prevent us from elaborating on these concepts, but the interested reader is referred to Ref [1] for more exhaustive explanations.

The principal difference between the two proposed CAPAM concepts is actually found in the Level Three models. Fault tree models like the one utilized in the FTB-CAPAM are in fact derived in terms of primary events representing component boolean failure states, whereas the LFM models of the NB-CAPAM describe a process in both success and failure spaces, via a fairly detailed representation of discretized process parameter states covering the actual parameter working range. Thus the former type of models will supply much less complete diagnostic information on disturbance root causes, and will not be able to provide indications for possible system recovery actions.

It is finally pointed out that, in order to assess actual system status, observable events in the CAPAM fault trees must be identified and "flagged" by corresponding combinations of alarm signals. This is because the majority of events in PRA-type fault trees represent component failure conditions that, unlike LFM network states, are not directly expressed in terms of observable parameter and variable values. Thus, even if the FTB-CAPAM developer can use PRA fault trees as a convenient start for his/her analysis, additional effort will have to be spent not only in restructuring the tree in the form most suitable for CAPAM utilization (e.g., with clear identification of safety function loss branches and parallel success path loss branches), but also in identifying alarms and alarm combinations that can be used as signals corresponding to events of interest and significance.

5. Signal Validation

CAPAM systems based on either of the two concepts presented herein will have to depend on process information

relayed to them by plant instrumentation. It is then sensible to consider the available options for on-line validation of instrument signals, to reduce the possibility of spurious system activations and false diagnoses. Use of "parity space" checking and fuzzy logic have been proposed as means of addressing this problem [3, 10].

The approach we propose here is a simplified version of the "parity space" method. It can be applied only when three or more redundant measures of the same quantity are available, although these need not be direct measures (but could be observed for instance from a reliable mass or energy balance). For each measured quantity a deviation tolerance is pre-established, and compared with the magnitude of the deviation of the i-th redundant measure of the given quantity from the average of all available measures. Measures whose deviations exceed the admitted tolerance are eliminated and the average based on the remaining measures is taken as the validated quantity measurement. For cases in which less than three measures were originally available, or less than two are left as a result of the above outlined procedure, the CAPAM analyses can be based on two alternative "menus". The first of these will be based on whatever average value is available, the second on the opposite assumption that no measure of the quantity can be considered reliable and that therefore the quantity must be considered presently unknown. The plant operators will thus be able to see the different "conclusions" that may be reached depending on whether an uncertain measure is accepted or not. A pre-selection of parameters to which to apply this procedure may be necessary to avoid an exponential growth of available menus: if for example a disturbance involved three uncertain measurements and the menu approach were unrestricted, the CAPAM could produce a possible maximum of eight different analyses, a result probably not very helpful to the operators.

6. Probability Margin Evaluations

Besides the types of operator assistance functions discussed in the previous sections, either CAPAM concept can provide an on-line quantitative evaluation of the probabilistic margins existing before the loss of any given safety function. Since each safety function is represented in either of the CAPAM Level Two representations essentially as a parallel of alternative success paths, the probability of OSF loss is given by the product of the alternative success path loss probabilities. When any of these are actually lost, and the loss is detected by the CAPAM, the corresponding probability terms in the OSF loss probability are set equal to 1. The OSF loss probability that results (which is obviously greater than the initial value corresponding to no success path loss) is then taken as the existing margin to loss of the given safety function.

In order to implement the outlined probability margin calculation, applicable values for the probabilities of success path loss must be collected and stored in the CAPAM models. If in addition one would desire to extend this kind of evaluation to cases in which there is only a partial failure within a success path but the success path is not yet lost, the probability quantification required would be much more extensive, as it would have now to cover failures of individual components or subsystems, rather than success paths as a whole. More details on this subject can be found in Ref. [1]. The point to be made here is that a probability margin evaluation capability can be built into the CAPAM rather easily if it is kept within a realistic scope. A more extended capability, covering component failures in great detail and accounting also for all possible kinds of dependencies in system and success path failures would obviously require a much greater effort.

7. Conclusions

Two alternative CAPAM concepts have been defined and outlined in this paper. The techniques that can be employed in their construction and implementation present a choice between an approach utilizing fault trees, like in "traditional" PRA analysis, or LFM graph based models. The former may be easier to develop, as they can be borrowed from available PRA analyses, but require "flagging" by alarms for event detection and require large amount of computer memory. The latter represent a more efficient and powerful tool for process modeling purposes and allow not only detailed diagnosis but also the identification of corrective actions at the subsystem level.

Being a relatively new tool, they may however be expected to require a learning period by unfamiliar analysts, and possibly more fine tuning and testing before implementation.

Regardless of the choice of tools and diagnostic ability to be built into a CAPAM system, a multi-level structure based on application of the concept of "safety functions" was found appropriate to meet the more general and essential system functional requirements. Possible solutions have also been developed on how to validate instrument signals to be used by the system, and how to calculate on-line probabilistic safety margin indications.

References

[1] S. B. Guarro, J. Szabo, D. Okrent: "Multi-Level Approach for Structural Definition of a Plant Wide DAS", UCLA-ENG-8424, September 1984.
[2] William R. Nelson: "Response Trees for Nuclear Reactor Operations", NUREG/CR-3631 (EGG-2293), February 1984.
[3] Alan M. Christie: "DICON: An Expert System Approach to Diagnostics and Control Guidance with LMFBR Application", WARD-SR-94000-37, October 1982.
[4] W. R. Corcoran et al.: "The Critical Safety Functions and Plant Operation", Nuclear Technology, Vol. 55, December 1981.
[5] S. Guarro, D. Okrent: "The Logic Flowgraph: A New Approach to Process Failure Modeling and Diagnosis for Disturbance Analysis Applications", Nuclear Technology, Vol. 67, December 1984.
[6] S. Guarro, D. Okrent: "Logic Flowgraph for Disturbance Analysis of a PWR Pressurizer System", International Meeting on Thermal Reactor Safety, Karlsruhe, West Germany, September 10-13, 1984.
[7] A. Madrid, S. Guarro: "Current Issues and Trends in the Use of Simulation in Nuclear Power Plant Disturbance Analysis Systems", International Conference on Power Plant Simulation, Cuernavaca (Mexico) November 19-21, 1984.
[8] "Using PRA to Assess Nuclear Power Plant Operating Events", Nuclear Safety Analysis Center, NSAC/54, August, 1982.
[9] "Combustion Engineering Emergency Procedure Guidelines", C-E Owners Group, CEN-152, November 1982.
[10] "On-Line Power Plant Signal Validation Technique Utilizing Parity-Space Representation and Analytic Redundancy", EPRI-NP-2110, November 1981.

Acknowledgements

This work was partially supported by a contract with the Japanese Atomic Energy Research Institute.

Table I: OSF threat severity ranking criterion.

No. of unavailable success paths (out of n possible)	Threat severity ranking	OSF CRT-window color
n	4	red
n-1	3	purple
from 2 to n-2	2	yellow
1	1	gray
0	0	green

Table II: Level-Two model structure.

OSF	Plant State	Success Path	Level-Two Systems Truth Table			Level-Two Parameters Truth Table	
PEMIC	A (At power)	A1	Prszr. Heaters	Prszr. Sprays	Level Contr. Sys.	Preszr. Pressure	Preszr. Level
		A2	PORVs		Level Contr. Sys.	Preszr. Pressure	Preszr. Level
	B (Shutdown with pressure or level excursion)	B1	PORVs		Safety Injection	Preszr. Pressure	Preszr. Pressure
		B2	Safety Valves		Safety Injection	Preszr. Pressure	Preszr. Pressure
	. . .	. . .	. . .			. . .	

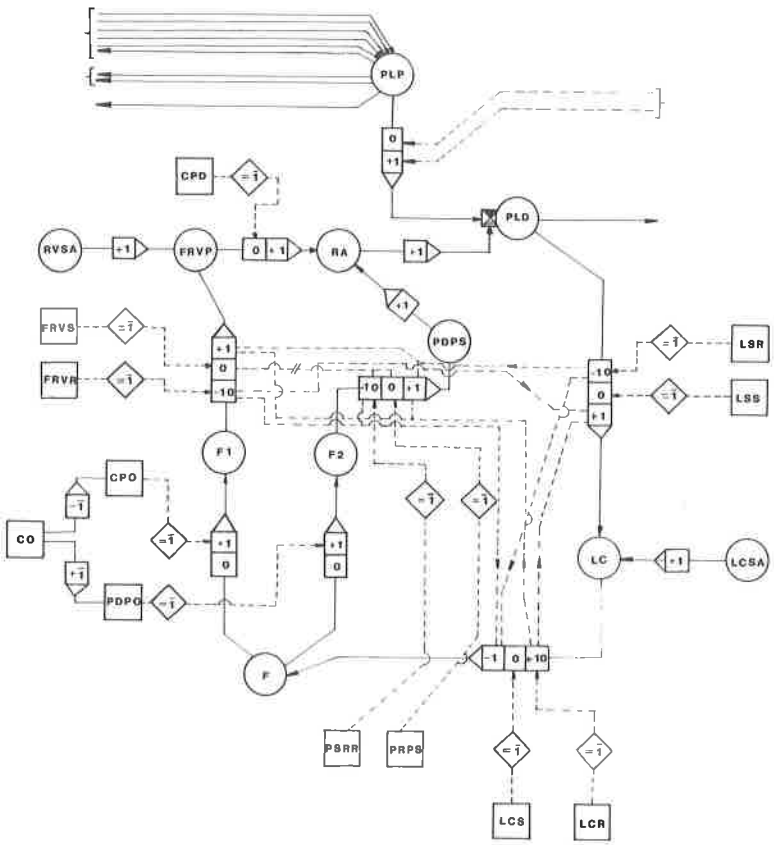

Figure 1: Example of Level-Three LFM Model